REMARKS

Claim Rejections - 35 USC §102

The examiner rejected claims 1-5, 7, 9, and 11-17 under 35 USC §102(e) as anticipated by Alonso et al. (6,434,700). The applicant respectfully disagrees.

Regarding claim 1, Alonso does not disclose or suggest to implement network authentication facilities within a disk drive. In particular, Alonso does not disclose or suggest a disk drive for receiving personal authentication data and user access data from a system administrator, or a disk drive comprising cryptographic circuitry for encrypting the user access data into encrypted data stored on a disk. In contrast, Alonso discloses a conventional Access Control Server (ACS) 202 for performing the network authentication facilities. Referring to FIG. 2 and col. 6, lines 62+, the ACS executes a number of precompiled software modules to implement, for example, Fortezza passwords. The ACS is connected to a database 204 (e.g., a disk drive) which stores user access data (col. 7, lines 16-24); however, the database 204 does not implement the network authentication facilities.

Alonso therefore discloses the same prior art network authentication implementation as shown in FIG. 1 of applicant's specification. The problem with this implementation, as described on page 3, lines 22+, is that an ACS is susceptible to physical probing attacks as well as remote virus attacks since the access control management is performed by a conventional operating system running on a conventional central processing unit (CPU). The invention recited in claim 1 overcomes this drawback by implementing the network authentication facilities within a disk drive. Since nothing in Alonso discloses or suggests this modification to the prior art, the rejection should be withdrawn.

The examiner asserts that Alonso discloses a Fortezza crypto card for implementing network authentication facilities. However, a Fortezza crypto card is not a

disk drive. Further, a Fortezza crypto card merely executes a hashing algorithm to generate a password from user access information. The password and user access information are then sent to a network access server which implements the network authentication facilities (col. 3, lines 22-35). Since a Fortezza crypto card is not a disk drive implementing network authentication facilities, the rejection should be withdrawn.

Regarding claims 2, 3, 4, 5, 7, 9 and 11, the examiner relies on the teaching by Alonso to use an access control server (ACS) to implement the network authentication facilities recited in the claims. However as described above, implementing network authentication facilities in a conventional authentication server has drawbacks which are overcome by encapsulating the implementation in a disk drive. The rejection should therefore be withdrawn.

Claim 12 recites a computer network comprising a plurality of interconnected network devices including a disk drive connected to an authentication server, wherein the disk drive comprises an interface for receiving from a client computer a user ID and a user access request to access a network device, and for transmitting device access data to the client computer. The disk drive further comprises cryptographic circuitry for decrypting data stored on a disk, wherein the decrypted data is used to generate device access data transmitted to the client computer.

Alonso does not disclose or suggest these limitations. In contrast, Alonso discloses a conventional access control server (ACS) for generating and transmitting the device access data to a client computer. As describe above, implementing network authentication facilities in a conventional authentication server has drawbacks which are overcome by encapsulating the implementation in a disk drive. The rejection should therefore be withdrawn.

The rejection of claims 13, 14, 15, 16, and 17 should be withdrawn for the reasons set forth above.

Claim Rejections - 35 USC §103

The examiner rejected claims 6, 8, 10, and 18-26 under 35 USC §103(a) as unpatentable over Alonso in view of DeTreville (6,609,199). The applicant respectfully disagrees.

Claim 22 recites a disk drive comprising an interface for receiving an encrypted device access request and for inputting/outputting user data from/to a client computer. The disk drive further comprises an internal drive key and an encrypted secrete device key shared with an authentication server. Cryptographic circuitry in the disk drive decrypts the encrypted secrete device key using the internal drive key to generate a decrypted secrete device key. The disk drive comprises an authenticator for authenticating the device access request using the decrypted secrete device key.

The examiner asserts that because DeTreville teaches the use of a secrete device key, the authorization access server disclosed by Alonso could be modified to include a secrete device key. However, modifying Alonso in view of DeTreville would result in an authentication server implementing network authentication facilities using a secrete device key and not a disk drive implementing authentication facilities using a secrete device key. Further, DeTreville discloses in FIG. 3 a computer 118 for implementing authentication facilities using a secrete key and therefore does not disclose or suggest to implement authentication facilities within a disk drive. The rejection should therefore be withdrawn.

The rejection of the remaining claims should be withdrawn for the reasons set forth above.

CONCLUSION

In view of the foregoing remarks, the rejections under 35 USC §102 and §103 should be withdrawn. In particular, the relied upon prior art does not disclose or suggest to implement network authentication facilities within a disk drive. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 4/22/04 By: _____

Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

4/22/04 Howard H. Sheerin
(Date) (Print Name)

_____
(Signature)